A Review Regarding the Biometrics Cryptography Challenging Design and Strategies

Mohamed Soltane
Electrical Engineering & Computing Department, Faculty of Sciences & Technology
Yahia Fares University of Medea, Medea, Algeria
Ministry of Higher Education and Scientific Research (Mhesr)
soltane.mohamed@univ-medea.dz; soltane.mohamed.3099@gmail.com & xor99@hotmail.com

Lotfi Messikh
Electrical Engineering Department, Faculty of Engineering Sciences
University 20 August 1955 of Skikda, Skikda, Algeria

Abdelhalim Zaoui
Electrical Engineering Research Unit,
Military Poytechnics School , BP 17, Bordj-El-Bahri, Phone +213 (021) 86 34 69, Algiers, Algeria

Abstract

As the information age matures, a biometric identification technology will be at the heart of computer interaction with humans and the biosphere in which they reside. Hence, the reliable information security mechanisms are needed to combat the rising magnitude of identity theft. While cryptography is a powerful tool to achieve information security, one of the main challenges in cryptosystems is to maintain the secrecy of the cryptographic keys. Template protection techniques prevent stored reference data from revealing private biometric information and enhance the security of biometric systems against attacks such as identity theft and cross matching. A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. The fuzzy vault construct is a challenging biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. The helper data itself do not leak any information about the biometric template, yet contain sufficient information to align the template and query biometric accurately. This paper reviews the state of the art biometrics Cryptosystems from the Point of Challenging Designs Strategies.

Keywords: Security and privacy enhancement, biometric-based cryptography, fuzzy vault, helper data, template protection and challenging designs.

1. Introduction

Cryptography (Grindlay, 2003) (derived from the Greek words *kryptos* and *graphein* meaning *hidden writing*) is the science of codes and ciphers. A cipher is essentially a cryptographic algorithm which is used to convert a message, known as the plaintext, into unreadable cipher-text. Cryptography is the science of using mathematics to encrypt and decrypt data (*An Introduction to Cryptography*, 1999-2000). Conventional cryptography uses encryption keys, which are just bit strings long enough, usually 128 bits or more. These keys, either "symmetric," "public," or "private," are an essential part of any cryptosystem, for example, Public Key Infrastructure (PKI). A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker. On the other hand, biometrics provides a person with unique characteristics which are always there. Can they be used as a cryptographic key? Unfortunately, the answer is negative: biometric images or templates are variable by nature, i.e., each new biometric sample is always different. Needless

to remind that conventional cryptography does not tolerate a single bit error. A biometric system always produces a Yes/No response, which is essentially one bit of information. Therefore, an obvious role of biometrics in the conventional cryptosystem is just password management. Upon receiving yes response, the system unlocks a password or a key. The key must be stored in a secure location (so called "trusted" device) (Cavoukian & Stoianov, 2007).

2. Motivations

What is Biometric Encryption? Biometric Encryption (Cavoukian & Stoianov, 2007) is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification. The digital key (password, PIN, etc.) is randomly generated on enrollment, so that the user (or anybody else) does not even know it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called "private template." In essence, the key *is encrypted* with the biometric. The BE template provides an excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrollment, both the key and the biometric are discarded.

Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits per pixel has 300x400x8 = 960,000 bits of information. Of course, this information is highly redundant. One can ask a question: Is it possible to consistently extract a relatively small number of bits, say 128, out of these 960,000 bits? Or, is it possible to bind a 128 bit key to the biometric information, so that the key could be consistently regenerated? While the answer to the first question is problematic, the second question has given rise to the new area of research, called Biometric Encryption (BE).

On verification, the user presents her fresh biometric sample, which, when applied to the Legitimate BE template, will let the BE algorithm retrieve the same key/password. In other words, the biometric serves as a *decryption key*. At the end of verification, the biometric sample is discarded once again. The BE algorithm is designed to account for acceptable variations in the input biometric. On the other hand, an attacker, whose biometric sample is different enough, will not be able to retrieve the password. This encryption/decryption scheme is *fuzzy*, as the biometric sample is different each time, unlike an encryption key in conventional cryptography (Cavoukian & Stoianov, 2007).

Current State of Biometric Encryption

The original concept of Biometric Encryption for fingerprints was pioneered in 1994 by Dr. George Tomko (Cavoukian & Stoianov, 2007), founder of Mytec Technologies (Toronto, Canada). Since then, many research groups have taken part in the development of BE and related technologies. There are about 50 articles and patents published to date, most of which appeared since 2002. Besides Biometric Encryption (BE), other terms have been used for this technology, such as: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, and bioHashing. BE and related technologies have drawn attention from major academic research centers specializing in biometrics, such as Michigan State University, West Virginia University, Carnegie Mellon University, University of Cambridge (U.K.), and University of Bologna (Italy). Among current industry leaders, those worth noting include IBM T.J. Watson Research Center, RSA Laboratories, Lucent Technologies, Sandia National Laboratories, and Philips

Research (Cavoukian & Stoianov, 2007).

Virtually all types of biometrics have been tested to bind (or to generate) a digital key: fingerprints, iris, face, keystroke dynamics, voice, handwritten signatures, palm-prints, acoustic ear recognition. The most promising results have been achieved with an iris: FRR = 0.47%, FAR = 0 (or at least less than one in 200,000) to generate a 140-bit key. These error rates are only marginally larger than for a conventional iris-based biometric system with the same input images. The use of fingerprints is also feasible in terms of accuracy for BE, with FRR greater than 10% at present. Unlike an iris, there is a noticeable degradation in accuracy from a conventional fingerprint system. This is understandable since fingerprints are more prone to distortions and other factors that degrade accuracy. It is more difficult to compensate those factors in the case of Biometric Encryption, since BE works in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). There are several ways to overcome this problem, for example, by using a free air (i.e., contactless) fingerprint sensor, or by using more than one finger from the same person, or by combining several biometrics (Cavoukian & Stoianov, 2007). Face recognition, which is usually considered third (after irises and fingerprints) in terms of accuracy in conventional biometrics, has shown a significant improvement of performance over the last few years. This allowed Philips Research to create a working BE system using a face biometric. The published results range from FRR = 3.5% for a face database with low to medium variability of images to FRR = 35% for a database with high variability; FAR = 0 (or at least less than 1 in 100,000) in both cases. The key size used is 58 bits, which may be sufficient as a password replacement. According to communication from Dr. Michiel van der Veen of Philips Research, their technology, called privIDTM, is now operational and ready for deployment; in particular, it will be a part of an EU 3D Face project (WP2.5). To the best of our knowledge, the Philips system wills the first real life application of BE technology (Cavoukian & Stoianov, 2007).

It is not clear if other biometrics have enough entropy (i.e., the amount of non-redundant Information) in order to bind a sufficiently long key (e.g. 128 bit). This is an area of future research.

Some published works provide a general theoretical foundation for BE technologies from a cryptographic point of view. They prove that the system can be made secure against "brute force" search attacks. In other words, an attacker checks, at random, all possible combinations in order to retrieve a key (or a biometric). Like conventional cryptography, it is assumed that the attacker is fully familiar with the algorithm, and may have a template in hand, but does not have a proper biometric to unlock the secret (i.e., the key bound to the biometric).

Xuebing Zhou (Zhou, 2007) proposes a template protection algorithm that merges methods from cryptography, error correction coding and biometrics. The proposed methods are integrated into a 3D face recognition system and tested on the 3D facial images of the FRGC database. It is shown that the resulting binary vectors provide an authentication performance that is similar to the original 3D face templates. A high security level is achieved with reasonable false acceptance and false rejection rates of the system, based on an efficient statistical analysis.

Monther Rateb et al. (Enayah & Samsudin, 2007) proposes a technique to generate a public cryptographic key from user's voice while speaking over a handheld device and making use of the human intelligence to identify/authenticate the voice of the speaker and therefore use the voice as the public key. The generated public key is used to encrypt the transferred data over the open communication channel. The implementation of such a system on mobile phones resists any eavesdrop on phone calls, even from the service provider itself. The proposed protocol also eliminates the need for a trusted third party.

Marten van Dijk et al. (Dijk & Tuyls, 2005) extend the information theoretic secure constructions for biometrics to the computational setting. Based on semantically secure encryption, it introduces robust, fully private and secure biometric key distillation and

verification. The model incorporates an adversary with side information who has access to a database with reference information. Even though its schemes are based on a master key, no master key needs to be stored in biometric sensors. In its scheme it is possible to derive a polynomial number of keys from a single biometric and it shows how to renew keys in a secure and private way without additional interaction with the user.

Alper Kanak (Kanak, 2004) gives a brief explanation of biometric cryptography approaches and algorithms which use various biometric data. He basically touches the use of keystroke dynamics, speech and 2D biometric data (such as fingerprint, palm-print, face,...etc).

Anil K. Jain et al. (Jain, Nandakumar & Nagar, 2008) present a high-level categorization of the various vulnerabilities of a biometric system and discuss countermeasures that have been proposed to address these vulnerabilities. In particular, their paper focuses on biometric template security which is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting the template is a challenging task due to intra-user variability in the acquired biometric traits. It presents an overview of various biometric template protection schemes and discusses their advantages and limitations in terms of security, revocability, and impact on matching accuracy. A template protection scheme with provable security and acceptable recognition performance has thus far remained elusive.

Pim Tuyls et al. (Tuyls & Goseling, 2004) formulate the requirements for privacy protecting biometric authentication systems. The secret capacity C_s is investigated for the discrete and the continuous case. It presents, furthermore, a general algorithm that meets the requirements and achieves C_s as well as C_{id} (the identification capacity). Finally, it presents some practical constructions of the general algorithm and analyzes their properties.

Feng Hao et al. (Hao, Anderson & Daugman, 2006) propose the first practical and secure way to integrate the iris biometric into cryptographic applications. A repeatable binary string, which we call a biometric key, is generated reliably from genuine iris codes. A well-known difficulty has been to cope with the 10 to 20% of error bits within an iris code and derive an error-free key. To solve this problem, the error patterns within iris code were carefully studied and it was devised a two-layer error correction technique that combines Hadamard and Reed-Solomon codes. The key is generated from a subject's iris image with the aid of auxiliary error-correction data, which do not reveal the key, and can be saved in a tamper-resistant token such as a smart card. The reproduction of the key depends on two factors: the iris biometric and the token. The attacker has to procure both of them to compromise the key. It evaluated their technique using iris samples from 70 different eyes, with 10 samples from each eye. It found that an error-free key can be reproduced reliably from genuine iris codes with a 99.5% success rate. It can generate up to 140 bits of biometric key, more than enough for 128-bit AES. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations.

Ari Juels et al. (Jules & Sudan, 2002) describe a simple and novel cryptographic construction that we refer to as a fuzzy vault. A player Alice may place a secret value κ in a fuzzy vault and "lock" it using a set A of elements from some public universe U. If Bob tries to "unlock" the vault using a set B of similar length, he obtains κ only if B is close to A, i.e., only if A and B overlap substantially. In contrast to previous constructions of this flavor, possess the useful feature of order invariance, meaning that the ordering of A and B is immaterial to the functioning of the vault. As shown, the scheme enjoys provable security against a computationally unbounded attacker.

Yagiz Sutcu et al. (Sutcu, Li & Memon, 2007) Examine and show how to apply a recently proposed secure sketch scheme in order to protect the biometric templates. They consider face biometrics and study how the performance of the authentication scheme would be affected after the application of the secure sketch. They further study the trade-off between the

performance of the scheme and the bound of the entropy loss from the secure sketch.

Pina Bergamo et al. (Bergamo, D'arco, Santis & Kocarev, 2004) study a public key cryptosystem based on Chebyshev polynomials, which provides both encryption and digital signature. The cryptosystem works with real numbers and is quite efficient. Unfortunately, from their analysis it comes up that it is not secure. They describe an attack which permits to recover the corresponding plaintext from a given cipher-text. The same attack can be applied to produce forgeries if the cryptosystem is used for signing messages. Then, they point out that also other primitives, a Diffie-Hellman like key agreement scheme and an authentication scheme, designed along the same lines of the cryptosystem, are not secure due to the aforementioned attack. They close the paper by discussing the issues and the possibilities of constructing public key cryptosystems on real numbers.

A very distinguished research paper comes from Walter J. Scheirer et al. (Scheirer & Boult, 2007) on security analysis of leading privacy enhanced technologies (PETs) for biometrics including biometric fuzzy vaults (BFV) and biometric encryption (BE). The lack of published attacks, combined with various "proven" security properties has been taken by some as a sign that these technologies are ready for deployment. While some of the existing BFV and BE techniques have "proven" security properties, those proofs make assumptions that may not, in general, be valid for biometric systems. They review some of the other known attacks against BFV and BE techniques. They introduce three disturbing classes of attacks against PET techniques including attack via record multiplicity, surreptitious key-inversion attack, and novel blended substitution attacks.

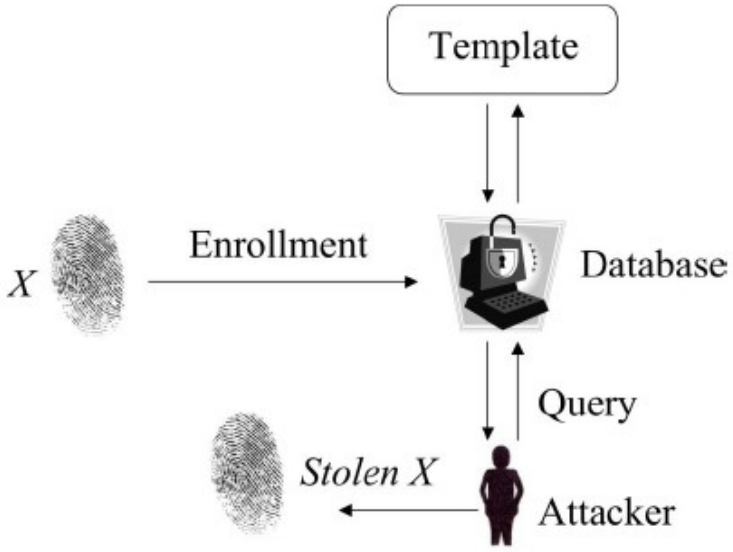


Figure 1 An attacker compromises the database, and is able to Retrieve the template X (Scheirer & Boult, 2007).

As depicted in Figure 1, a traditional biometric system will store the original templates in a database, for use in authentication/identification comparisons. If an attacker can gain access to the database (despite its security measures), all template data (X) can be compromised. Unfortunately, illicit access to databases with "private" information has become commonplace, with over 150 million financial/personnel records lost in 2006 (Scheirer & Boult, 2007).

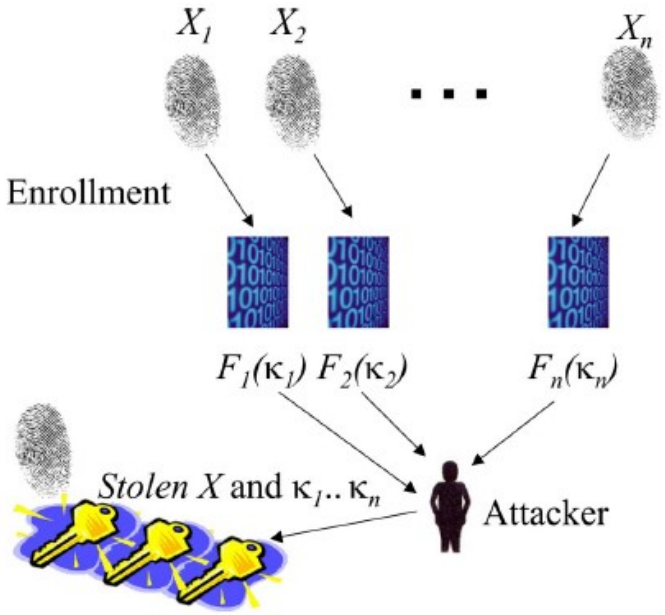


Figure 2 Attacks via Record Multiplicity (ARM). An attacker collects multiple enrollment templates, and is able to combine the data, at minimum link records, and in the most dangerous case can retrieve the template X and the secret κ (Scheirer & Boult, 2007).

Referring to Figure 2, multiple enrollments can be seen for the same set of biometric template data *X*. Each enrollment has its own secret κ, resulting in multiple different encodings $(F_1(\kappa_1) to F_n(\kappa_n))$. which are subsequently transmitted and stored by various systems with the same implementation. In an Attack via Record Multiplicity (ARM), if an attacker can harvest several of these encodings, it may be possible to correlate the data contained within, between encodings to link the databases or, in some cases to directly retrieve *X* and $\kappa_1 \dots \kappa_n$.

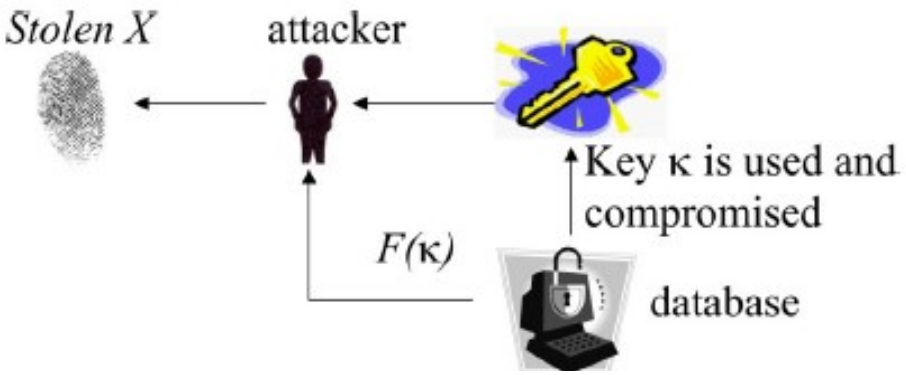


Figure 3 The SKI attack. If the attacker has knowledge of the secret κ, the template X can be recovered (Scheirer & Boult, 2007).

In BFV and BE, the stated goal of the system is the release of a secret key. To be useful, this key needs to be used for something, and if it leaves the vault in plain text form opens up a new range of attacks. Figure 3 shows this with encoded data *F(κ)* and an intercepted secret κ. By knowing κ, an attacker can decode the biometric template data *X* by identifying values related to κ.

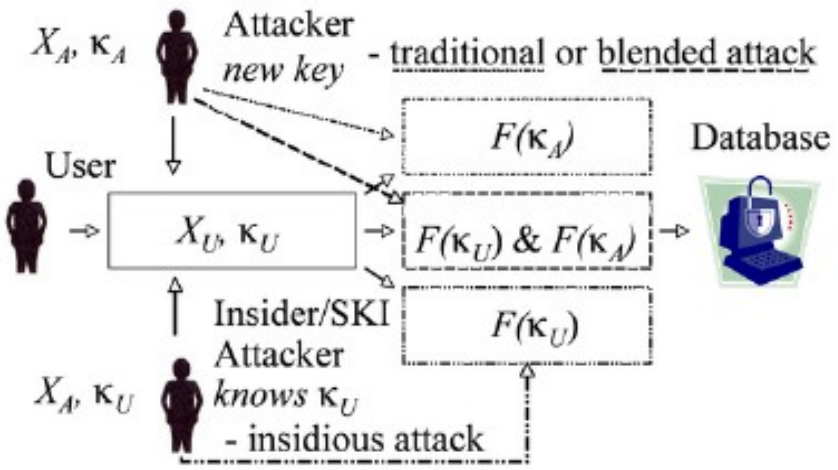


Figure 4 Traditional and blended substitution attacks (Scheirer & Boult, 2007).

In the new blended substitution (Figure 4), the user's and attacker's data are combined in a single template. If they blend using secret K_U it is called an *insidious blending* as there is no way to detect it is being used. A blended template allows either the user or the attacker to authenticate against the same record. In the traditional substitution case the attacker can authenticate but simultaneously produces a denial of service to the original user, which increases the chance of detection. In the new blended substitution the attacker can use the records simultaneously with the user (Scheirer & Boult, 2007).
At the end five requirements for secure biometric PETs architectures have been defined:

1. No combination of data from multiple enrollments by the same individual should be able to be combined to recover the biometric template data or to generate a spoof.
2. If any non-biometric data that is used to encode/decode (e.g. link table), or is released by the system (e.g. key), is known, the biometric template must not be recoverable nor should it allow hill-climbing or spoof generation.
3. It should not be possible for two users to authenticate against the same token with significantly higher frequency than the system's documented False Accept Rate.
4. No undetected substitution of records should be possible.
5. Any data transmitted outside the system, except during enrollment, should not be suitable to link the underlying user over space/time/companies.

Threats and Vulnerabilities for Biometric Systems

Biometrics-based personal authentication systems that use physiological (e.g., finger-print, face, iris) or behavioral (e.g., speech, handwriting) traits are being increasingly utilized in many applications to enhance the security of physical and logical access systems. Even though biometric systems offer several advantages over traditional token (e.g., key) or knowledge (e.g., password) based authentication schemes (e.g., increased user convenience and robustness against imposter users), they are still vulnerable to attacks. Andy Adler (Adler, 2005) describes a potential vulnerability in such systems, that allows a less-than-brute force regeneration of the secret and an estimate of the enrolled image. This vulnerability requires the biometric comparison to "leak" some information from which an analogue for a match score may be calculated. Using this match score value, a "hill-climbing" attack is performed against the algorithm to calculate an estimate of the enrolled image, which is then used to decrypt the code.

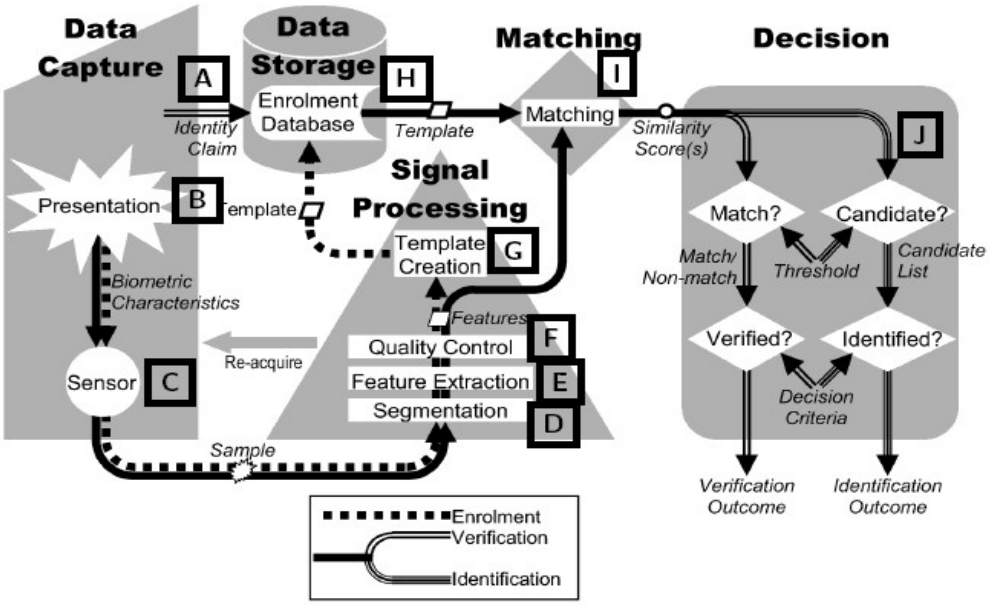


Figure 5 Vulnerabilities in Biometric Systems (Adler, 2008). Steps A - H are analyzed in section 2 (Adler, 2005). Each presented sample (B) is acquired by a sensor (C) processed via segmentation (D) and feature extraction (D) algorithms. If available, a sample quality (E) assessment algorithm is used to indicate a need to reacquire the sample. Biometric features are encoded into a template, which is stored (H) in a database, on an identity card or in secure hardware. For biometric encryption systems, a code or token is combined with the biometric features in the template. During enrollment, biometric samples are linked to a claimed identity (A), and during subsequent verification or identification, samples are tested against enrolled samples, using a matching algorithm (I) and an identity decision (J) is made, either automatically, or by a human agent reviewing biometric system outputs (Adler, 2008).

3. Biometrics Cryptosystems: Challenging Designs Strategies

Password-based authentication systems do not involve any complex pattern recognition and, hence, they almost always perform accurately, as intended by their system designers. The real challenge in biometric cryptosystems comes from the fact that biometric signal and their representations (e.g., facial image and their computer representation) of a person vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition device, and (in some cases) variation in the traits due to various pathophysiological phenomena. A lot of noise is introduced during data acquisition process. This same biometric may change between successive acquisitions (due to wound, ageing etc.) and noise can be introduced to a biometric signal by an acquisition device or the environment, while it is very convenient to use biometric traits for encryption. In its most basic sense, generating a cryptographic key directly from a biometric trait, for instance fingerprints, has not been very successful, as it involves obtaining an exact key from a highly variable data. The greatest challenge is to design cryptosystems that generate non linkable templates, provides good trade-off between accuracy & security and utilize feature adaptation schemes that preserve accuracy and allow easy fusion of modalities.

Biometric cryptosystems are classified as key release, key binding and key generation systems depending on how the secure sketch is obtained. Secure sketch is public information about biometric features stored in databases during enrollment. Fuzzy vault and fuzzy commitment are the two most popular techniques used for constructing biometric cryptosystems. Figure 6 shows an overview of template protection and related technologies.

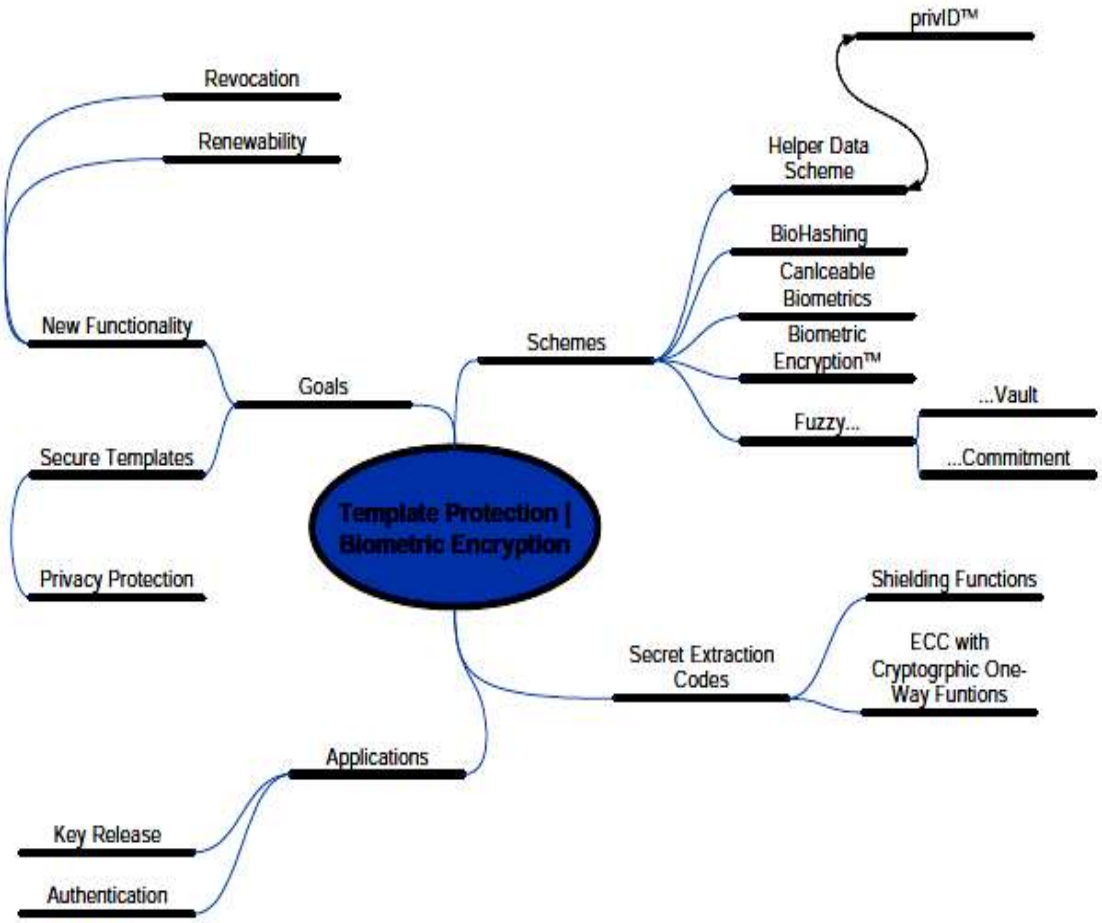


Figure 6. Overview of template protection and related technologies

3.1. Shielding Functions

Every measurement of a biometric modality is accompanied by noise. At enrollment X is assumed to be noiseless. To authenticate, in the sense of classical biometric verification approaches, X' needs to be matched against the reference X in a fuzzy manner using distance measurement and a decision based on a threshold. As renewability is to be realized, templates cannot be stored without any transformation. This transformation is done with the help of some random part S that is merged with the feature vector. This secret S can also be used as a standard cryptographic key, "fuzzy matching" of S is not possible. To deal with biometric data, the extraction of S must be resilient to noise.

Shielding Functions (Linnartz & Tuyls, 2003) fulfill this requirement. They form a set of *Secret Extraction Codes (SEC)* – secrets can be extracted correctly out of a dataset up to a certain level of noise. If G is such a function, it can be understood as:

$$G: \Re^k \times \{0,1\}^k \rightarrow \{0,1\}^K \qquad (1)$$

It is possible to extract a secret of length K with a biometric $X \in \Re^k$.

Some helper data $W \in 0, 1^k$ is needed here. W is computed in order to satisfy the term G(X,W) = S.

Shielding function has two properties:

- ✓ δ-*contracting* – For all biometrics X' that lie in a certain radius around X, the secret extracted with G, using the same helper data, is equal:

$$G(\mathbf{X}', W) = G(X, W) = S \qquad (2)$$

- ✓ ϵ *-revealing* – The information about S with knowledge of *W*, which can be sent over insecure channels, should be less than ϵ bits. It has been shown in (Linnartz & Tuyls, 2003) that ϵ cannot equal zero.

This scheme can be used to enroll and authenticate users. A trusted authority (*TA*) is needed, otherwise the biometric template or the secret could be compromised. The following steps are necessary for enrollment:

- ✓ Extract biometric *X* of the user *U* to enroll.
- ✓ Choose a random secret S.
- ✓ Compute helper data *W* out of *S* and *X*, erase *X* afterwards.
- ✓ Apply a one-way-function *h* on *S*, erase *S*.
- ✓ Store dataset [*U, W, h(S)*] for user *U* in database.

Figure 7 illustrates Principles of privacy protecting systems and Figure 8 illustrates an enrollment process incorporating shielding functions.

To verify the identity of user *U*, the secret is recalculated and compared bit-wise with the stored reference created in the enrollment phase:

- ✓ Measure the noise-afflicted *X′* of user *U*.
- ✓ Dataset for claimed identity *U* is loaded.
- ✓ W is used to compute *S′= G(X′,W)*.
- ✓ Compute h(S′) and compare it with h(S).
- ✓ Verification is successful if both values are identical, otherwise the user is rejected.

If $|G(X', W) - G(X, W)| \leq \delta$ the secret is mapped to the same point in the space.

The principle workflow is nearly the same for the different schemes of privacy protection. The concrete implementation depends on the chosen biometric modality the system was designed for and on preferences of the publishers.

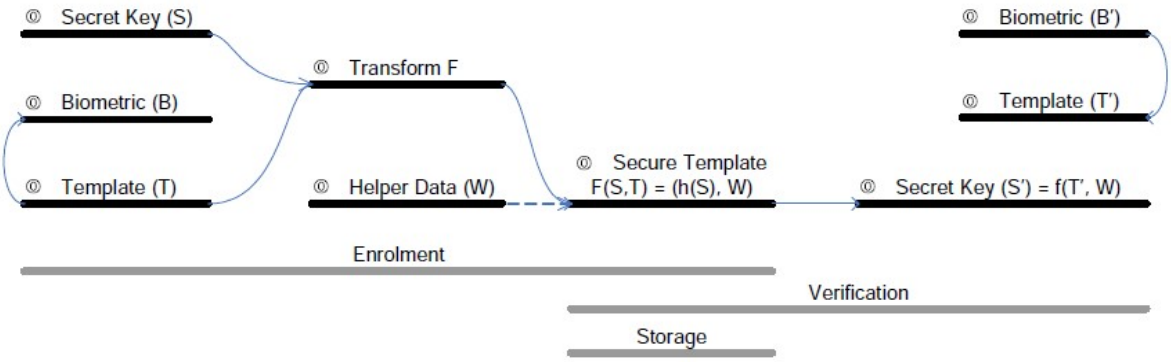
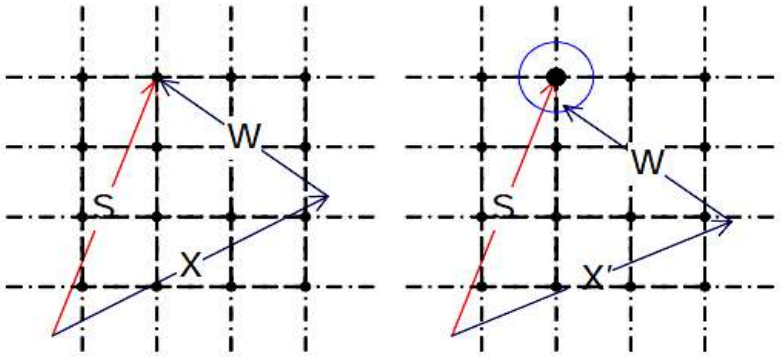


Figure 7. Principles of privacy protecting systems



(a) Enrolment with shielding (b) Positive verification with X' functions

Figure 8. Illustration of the basic principle of shielding functions: Each grid-point stands for one possible secret word that can be encoded. The circle is an abstraction of the δ-area around the secret S, in which S can be decoded properly.

3.2. Fuzzy Commitment

Fuzzy Commitment was introduced by Juels and Wattenberg (Juels & Wattenberg, 1999) as "... a new type of cryptographic primitive". One goal is the secure commitment of an embedded value. This secret value can only be regained with a decryption key named "witness", that it is close to the one used for concealing. Hence results the name "fuzzy". Therefore the system qualifies for securing keys with biometric data. It will be seen that the biometric information does not need to be stored for authentication purposes, which implies the possibility to create secure templates. Some kind of shielding function is used to provide the required functionality.

A Fuzzy Commitment Scheme *F* consists of a codeword *c* and a witness *x*, both having the same size of *n-bits*. The idea is to express x as an addition of c and helper data *δ*. The codeword is sealed with a one-way function h, *δ* remains untouched and can be used to provide resilience to *x*. The amount of information sealed in *h(c)* depends on the number of possible codewords $|c| = 2k$, for higher values of *k* the security of the system will improve. Helper data *δ* can be seen as the degree of resilience in *F*. To take a more concrete look at the system: Let *h* be a hash function mapping discrete values $\{0,1\}^n \rightarrow \{0,1\}^l$.

$$F: (\{0,1\}^n, \{0,1\}^n) \rightarrow (\{0,1\}^l, \{0,1\}^n) \text{ is defined as: } F(c,x) = (h(c), x-c) = (\alpha,\delta) \quad (3)$$

The receiver of *(α, δ)* can re-compute the codeword if he possesses a witness x'. Therefore a decoding function called *f* is needed that maps values x^i to the nearest possible codeword:

$$f(x' - \delta_i) = c_i, \forall c_i \in \{0,1\}^n, x' \in \{0,1\}^n \; \forall a: |\delta_i| < |\delta_a| \quad (4)$$

To unlock the secret c the helper data has to be subtracted from the noisy witness.

$$f(c + (x' - x)) = f(x' + \delta) = c' \quad (5)$$

If $h(c) = \alpha$, c' is the correct commitment.

Applied on biometric authentication systems the enrollment phase consists of three steps:

- ✓ User *U* presents the biometric *x*
- ✓ A codeword *c* is chosen randomly
- ✓ The Fuzzy Commitment $y_U - F(c, x)$ is calculated and stored associated to user *U*

At the beginning of the verification phase the biometric *x′* of user U is taken. If the commitment can be successfully computed, the user is authenticated because its submitted characteristic is close enough to the original reference template.

Fuzzy Commitment is also capable of forming a challenge-response authentication system based on public key cryptography:

Enrollment – The codeword *c* is used to create a pair of a secret- and a corresponding public key. The user *U* stores *F(c, x),* the public key is registered at a trusted authority (*TA*).

Verification – To authenticate against the *TA*, a random message m is sent to the user *U*. If *U* can answer this message with a valid signature of *m*, he or she is authenticated because the possession of the private key is proven (which can be checked by the *TA* with the registered public key).

To realize an **encryption system**, the user has to choose c as a symmetric cryptographic key that can be released with the biometric *x′*. To encrypt a message *m* the struct $(E_c(m), F(c, x))$ has to be stored.

3.3. Fuzzy Vault

Another system for storing secure templates is Fuzzy Vault from Juels and Sudan (*An Introduction to Cryptography*, 1999-2000; Cavoukian & Stoianov, 2007; Zhou, 2007) from 2002. The convenience of biometrics is combined with the security of cryptography. A biometric template or an unordered set $X = \{x_1, x_2, \ldots, x_n\}$ is used to secure a key $K = \{k_1, k_2, \ldots, k_n\}$.

A polynomial $p(X) = \sum_{i=n}^{1} k_i x^{i-1}$ is constructed – its coefficients are equal to the components of the key. The template *X* is transformed with our polynomial, some randomly generated points that do not lie on *p* are added to a set *R*. These "chaff points" should hinder attackers to reveal both the key and the feature vector.

The secure template contains *R* and *h(K).* To release *K*, another feature vector X' is extracted from a presented biometric characteristic. If *X* and X' overlap substantially the original polynomial can be recomputed – many points in *R* and R' are equal. Otherwise if a certain degree of similarity of the features is not given, solving this problem is hard (*polynomial reconstruction problem*). Error correction techniques enable to regain K even if the biometric characteristic used for unlocking is disturbed by noise.

An example illustrates this scheme:

- ✓ The biometric is defined by *X = {2,−1, 5,−2}*. Remember that this set is unordered.
- ✓ Forming the polynomial is done regarding to *K = {−3, 2, 1}:*

$$p(X) = x^2 + 2x - 3$$

- ✓ As a result the projection is available

$$p(X) = \{(2,5); (-1,-4); (5,32); (-2,-3)\}$$

- ✓ Chaff point $C = \{(0, 2); (3,-1)\}$ is added to a new set $R = p(x) \cup C$

- ✓ If the user can separate at least three points out of

$$R = \{(2, 5); (0, 2); (-1,-4); (5, 32); (3,-1); (-2,-3)\}$$

The polynomial and therefore K can be found – if the degree is i, the polynomial can be defined exactly with the knowledge of $i + 1$ points laying on it.

3.4. Key Binding Biometric Cryptosystems

In a key-binding cryptosystem, the biometric template is secured by monolithically binding it with a key within a cryptographic framework. A single entity that embeds both the key and the template is stored in the database as helper data. This helper data does not reveal much information about the key or the biometric template, that is, it is computationally hard to decode the key or the template without any knowledge of the user's biometric data. Usually the helper data is an association of an error correcting code (selected using the key) and the biometric template. When a biometric query differs from the template within certain error tolerance, the associated codeword with similar amount of error can be recovered, which can be decoded to obtain the exact codeword, and hence recover the embedded key. Recovery of the correct key implies a successful match. Figure 9 illustrates the basic concept of Biometric Key-Binding.

Advantages

- ✓ This approach is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword.

Limitations

- ✓ Matching has to be done using error correction schemes and this precludes the use of sophisticated matchers developed specifically for matching the original biometric template. This can possibly lead to a reduction in the matching accuracy.

- ✓ In general, biometric cryptosystems are not designed to provide diversity and revocability. However, attempts are being made to introduce these two properties into biometric cryptosystems mainly by using them in conjunction with other approaches such as salting (Boyen, 2004; Boult et. al., 2007; Nandakumar et. al., 2007).

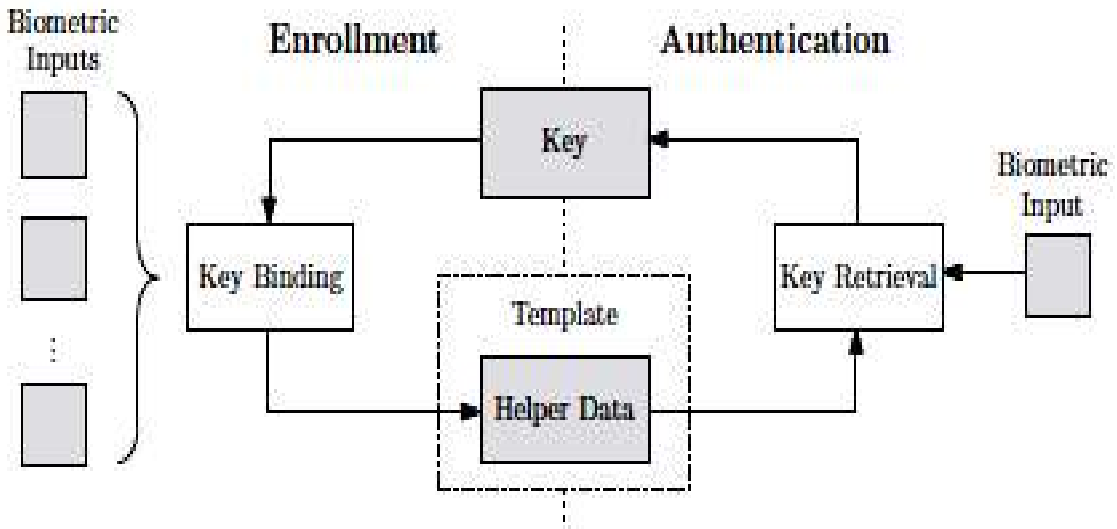


Figure 9. The basic concept of Biometric Key-Binding

3.5. Key Release Based on Biometrics

The cryptographic key is stored to database as user records. After successfully biometric based authentication, key is used. In this case, security of system depends on biometric authentication. However, the cryptographic key's entropy and randomness characters are very high and changing this case is very easy. The characteristics of the biometric key release system design are:

- ✓ It requires access to biometric templates for biometric matching.
- ✓ User authentication and key release are completely decoupled.

Because the system stores biometric template locally, the design raises concerns about the theft of biometric data. Figure 10 illustrates the basic concept of Biometric (a) Key-Binding and (b) Key-Release (Zhe, Andrew, Bok-Min & Yong-Haurt, 2016).

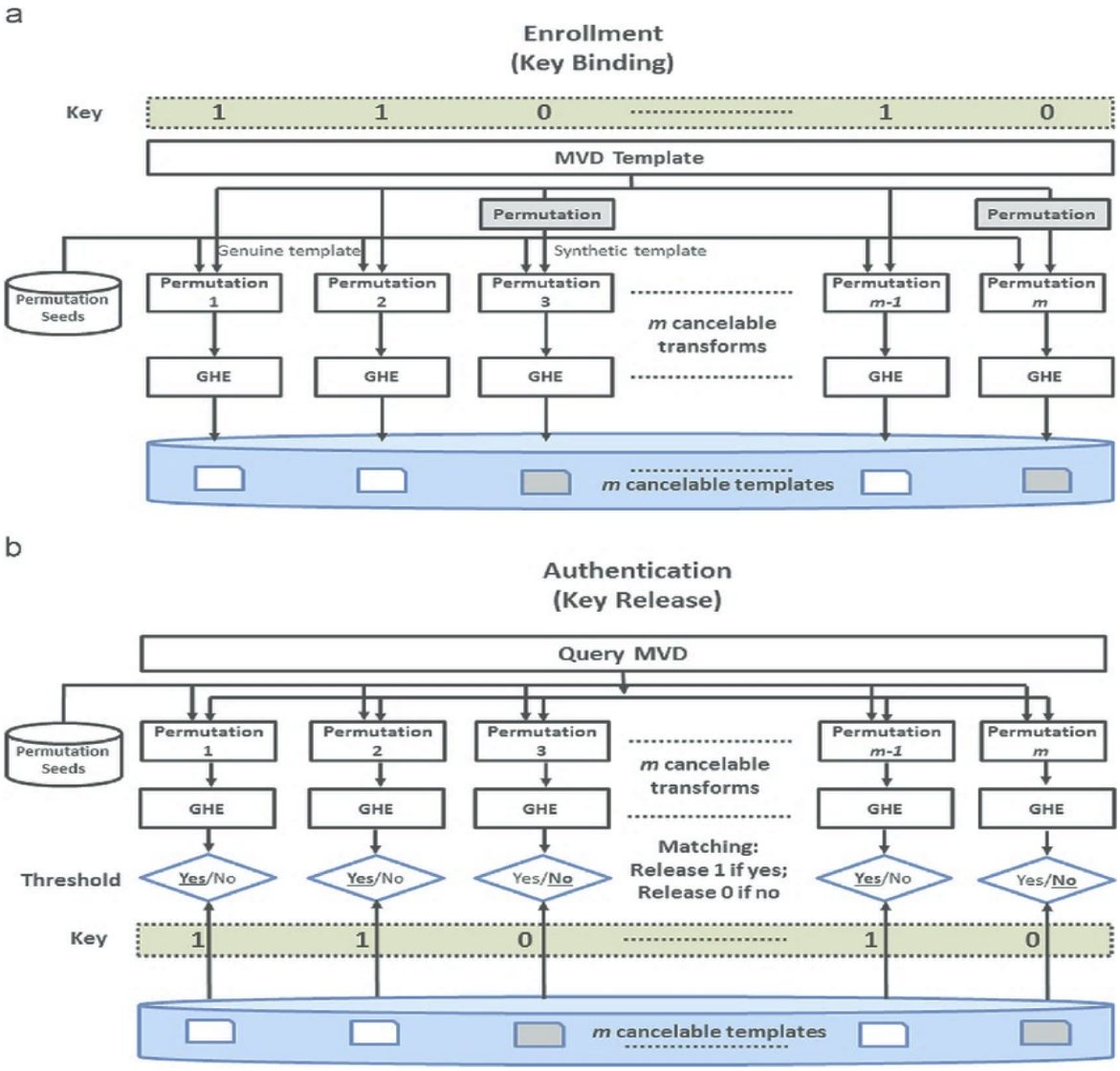


Figure 10. The basic concept of Biometric (a) Key-Binding and (b) Key-Release (Zhe et. al., 2016)

3.6. Key Generation Biometric Cryptosystems

In this scheme, helper data are derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample. Generated key's entropy is not high and updating this key is difficult. This scheme is also based on error correction code. Fuzzy extractor and secure sketch are referred as key generation schemes. Figure 11 illustrates the basic concept of Biometric Key-Generation.

BKGs (biometric key generators) are generally composed of two algorithms, an enrollment algorithm (**Enroll**) and a key-generation algorithm (**KeyGen**):

- $\mathbf{Enroll}\ (\beta_1, \ldots, \beta_l)$: The enroll algorithm is a probabilistic algorithm that accepts as input a number of biometric samples $\mathbf{Enroll}\ (\beta_1, \ldots, \beta_l)$, and outputs a template ($\mathcal{T}$) and a cryptographic key ($\mathcal{K}$). In the event that $\mathbf{Enroll}\ (\beta_1, \ldots, \beta_l)$ do not meet some predetermined criteria, the enroll algorithm might output the failure symbol $\perp$.
- $\mathbf{KeyGen}\ (\beta, T)$: The key generation algorithm accepts as input one biometric sample (β),

and a template (T). The algorithm outputs either a cryptographic key (K), or the failure symbol $\perp$ if **β** cannot be used to create a key.

The enrollment algorithm estimates the variation inherent to a particular user's biometric reading and computes information needed to error-correct a new sample that is sufficiently close to the enrollment samples. **Enroll** encodes this information into a template and outputs the template and the associated key. The key-generation algorithm uses the template output by the enrollment algorithm and a new biometric sample to output a key. If the provided sample is sufficiently similar to those provided during enrollment, then **KeyGen** and **Enroll** output the same keys.

Generally speaking, there are four classes of information associated with a BKG:

- ***The Biometric (β):*** A biometric is a measurement of a person's behavior or physiology. A BKG extracts **β** as algorithmically interpretable representations (e.g., a set of signals). The BKG typically applies statistical functions, or features $(\Phi_1, \ldots, \Phi_n)$, to the representations, and uses the output to either derive or lock a cryptographic key (Soutar et. al., 1998; Hao & Wah, 2002; Uludag & Jain, 2006; Wayman, 2001; Vielhauer et. al., 2002; Hao et. al., 2006).
- ***A Template (T):*** A template is any piece of information that is stored on the system for the purpose of re-generating the cryptographic key. Templates are generally created during an enrollment process and stored so that a user can easily recreate her key. For all practical purposes, templates must be considered publicly available. Note that this assumption implies that more standard biometric templates, which are typically employed for authentication purposes and are simply the encoding of a biometric, cannot be used securely in this setting (Soutar et. al., 1998; Hao & Wah, 2002; Uludag & Jain, 2006; Wayman, 2001; Vielhauer et. al., 2002; Hao et. al., 2006).
- ***The Key (K):*** A cryptographic key that is derived from (or locked by) one or more biometric samples during an enrollment phase. The key may later be regenerated using another biometric sample that is "close" to the original samples and the template that was also output during enrollment (Soutar et. al., 1998; Hao & Wah, 2002; Uludag & Jain, 2006; Wayman, 2001; Vielhauer et. al., 2002; Hao et. al., 2006).
- ***Auxiliary Information (A):*** Auxiliary information encompasses any public information not intended to be used for key-derivation purposes but that is still readily available to an adversary. Auxiliary information is specified with respect to one user and includes any biometric, template, or key, other than those associated with the user in question. It could also include any other information about the environment that might leak information about the biometric, or results of using the key (Soutar et. al., 1998; Hao & Wah, 2002; Uludag & Jain, 2006; Wayman, 2001; Vielhauer et. al., 2002; Hao et. al., 2006).

State of the art of Biometric Key Generation: Soutar and Tomko (Soutar & Tomko, 1996) were the first to describe a different approach for generating cryptographic keys from fingerprints using optical computing techniques. Fabian et al. (Fabian, Michael, Qi, & Susanne, 2001) propose a technique to reliably generate a cryptographic key from a user's voice while speaking a password. Davida et al. (Davida, Frankel, & Matt, 1998) proposed an approach that uses iris codes, which are believed to have the highest entropy of all commonly-used biometrics. Monrose et al. (Monrose, Reiter, Li, & Wetzel, 2001) proposed the first practical system that exploits behavioral (versus physiological) biometrics for key generation. Their technique uses keystroke latencies to increase the entropy of standard passwords. Their construction yields a key at least as secure as the password alone, and an empirical analysis showed that in some instances their approach increases the workload of an attacker by a

multiplicative factor of 2^{15}. Many constructions followed those of Monrose et al., using biometrics such as face, fingerprints, and handwriting. Unfortunately, many are susceptible to attacks. Hill-climbing attacks have been leveraged against fingerprint, face, and handwriting-based biometric systems by exploiting information leaked during the reconstruction of the key from the biometric template (Hao & Wah, 2002; Monrose et. al., 2002; Goh & Ngo, 2003; Uludag, 2004; Adler, 2004; Uludag & Jain, 2004; Vielhauer & Steinmetz, 2004; Yamazaki et. al., 2005; Zheng & Zhan, 2006).

Fuzzy cryptography (Jain, Ross, & Uludag, 2005) has made important contributions by specifying formal security definitions with which BKGs can be analyzed. Nevertheless, there remains a gap between theoretical soundness and practical systems. For instance, while fuzzy extractors can be effectively used as a component in a larger biometric key generation system, they do not capture all the practical requirements of a BKG. In particular, it is unclear whether known constructions can correct the kinds of errors typically generated by humans, especially in the case of behavioral biometrics. Moreover, fuzzy extractors require biometric inputs with high min-entropy but do not address how to select features that achieve this requisite level of entropy. Since this is an inherently empirical question, much of our work is concerned with how to experimentally evaluate the entropy available in a biometric. Lastly, Jain et al. (Jain, Ross, & Uludag, 2005) enumerate possible attacks against biometric templates and discuss several practical approaches that increase template security.

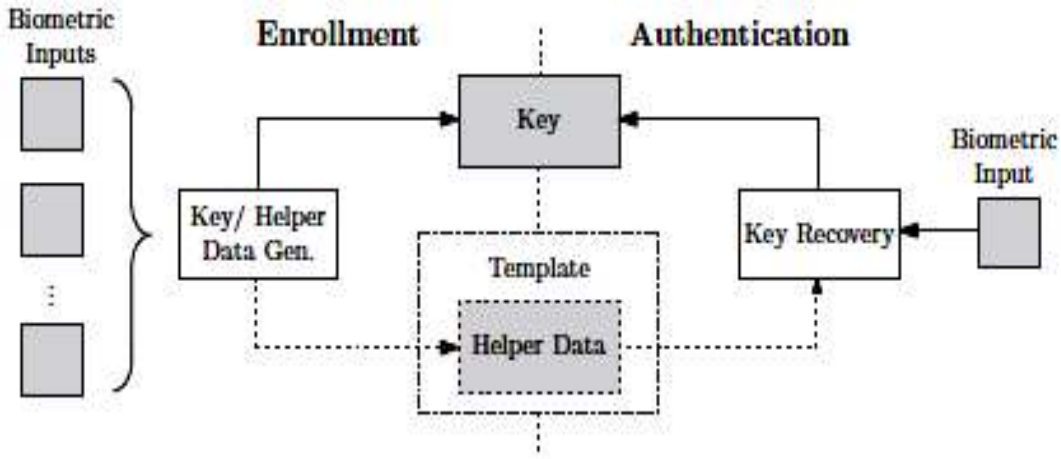


Figure 11. The basic concept of Biometric Key-Generation

3.7. Cancelable Biometrics

One of the advantages of passwords and tokens over biometrics is that they can be updated. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics to create a more secure system. Cancelable biometric transforms are designed in a way that it should be computationally hard to recover the original biometric data. It was first proposed by Ratha et al (Ratha, Connell, & Bolle, 2001). Two main categories of cancelable biometrics are distinguished: non-invertible transforms and biometric salting.

- **Non-invertible transforms:** In these approaches, biometric data are transformed applying a noninvertible function. In order to provide updatable templates, parameters of the applied transforms are modified. The advantage of applying noninvertible transforms is that potential impostors are not able to reconstruct the entire biometric

data even if transforms are compromised. However, applying non-invertible transforms mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align in order to perform a proper comparison and, in addition, information is reduced. For several approaches these effects have been observed (Ratha, Connell, & Bolle, 2001; Zuo, Ratha, & Connel, 2008). Figure 12 illustrates the diagram of Biometric Cancelable Templates from Different Transforms.

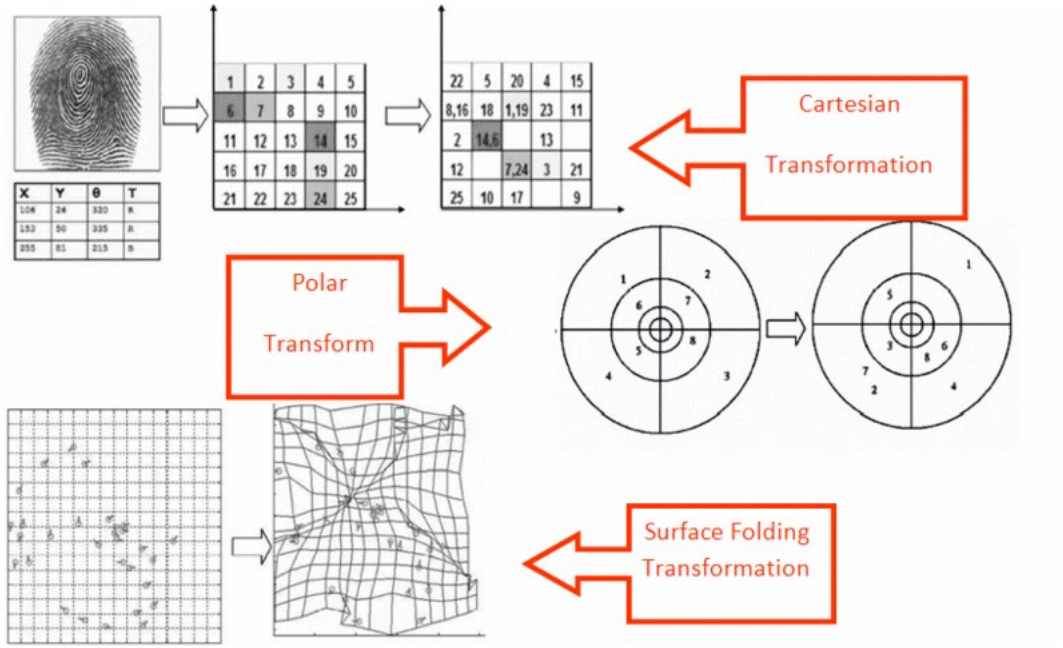


Figure 12. Cancelable Templates from Different Transforms (Ratha, Connell, & Bolle, 2001)

- **Biometric salting:** Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal (Savvides, Kumar, & Khosla, 2004). As a consequence, the parameters of the transformation have to be kept secret. In case user-specific transformations are applied, the parameters of the transformation (which can be seen as a secret seed (Teoh, Kuan, & Lee, 2008) have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transformation parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transformations. While approaches to biometric salting may maintain the recognition performance of biometric systems non-invertible transformations provide higher security (Jain, Nandakumar, & Nagar, 2008). Approaches to CB can be classified further with respect parts of biometric systems in which transformations are applied. In the signal domain, transformations are either applied to raw biometric measurements (e.g., face image - Ratha, Connell, & Bolle, 2001). In case transformations are applied in signal domain comparators do not need to be adapted. In feature domain extracted biometric features (e.g., face features in Teoh, Kuan, & Lee, 2008) are transformed, thus, a compromise of transformations requires further effort in reconstructing the original biometric from the template (Ratha, Connell, & Bolle, 2001; Teoh, Kuan, & Lee, 2008). Figure 13 illustrates the diagram of Biometric Salting.

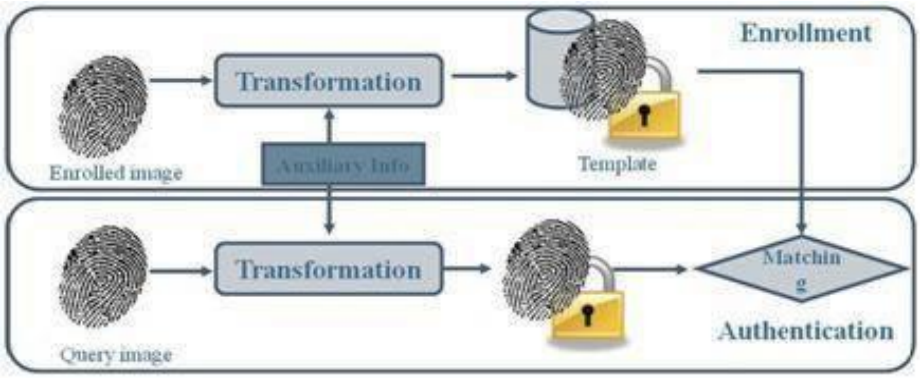


Figure 13. Block diagram of Biometric Salting

4. Conclusions and Future Visions

Skeptics may argue that many earlier attempts at using cryptography for user authentication have failed to displace passwords on the Internet! Its deep questions with practical significance; that Cryptography, which allows us to maintain secrecy in messages containing sensitive information, is based on requiring anyone other than an authorized person to perform a very difficult computation in order to steal the information. The current notions of difficulty are based on the classical algorithmic model. In the quantum world, many computations that are classically difficult are in fact easy tasks. Meanwhile the quantum age technology becomes mature to be handled and manipulated by human-beings at the level of elementary particles and subatomic technology.

Uncertainty principle, discovered and formulated in 1927 by Werner Heisenberg, states that certain pairs of values cannot both be known to arbitrary precision. That is, the measurement of one of the properties affects the system in such a way that part of information concerning the other value is lost. The uncertainty principle results from the nature of reality itself rather than form an imperfection of measuring methods or tools. The principle is a consequence of the wave-particle duality (Krzyszkowska-Pytel, 2010).

Quantum information means a state of an object in a quantum sense (e.g. the state of a particle is described by its wave function) which is unobservable for classic objects, and which communicates with other systems in a quantum way. Quantum information is processed in a way that is unreadable to a classic observer. When measuring quantum systems a "classic observer" can read "classic information" contained therein. However, this is possible only to a little degree given the whole content of quantum information contained in the system concerned. Uncertainty principle is the barrier as any measurement of one value disturbs the quantum state in such a way that it becomes impossible to measure another value. Quantum systems have enormous capacities. The capacities grow exponentially with the number of particles, whereas classic information which is readable for a classic observer grows with the number of particles only in a linear way (just like in the classic information technology) (Krzyszkowska-Pytel, 2010).

DNA biometrics code digital information concerning identity contained in a cell. So far this method has been used in forensic medicine. Its most considerable disadvantage is the fact that monozygotic twins have identical DNA. It is also a very expensive, complicated and slow method. Quantum cryptography and DNA biometrics can be combined by following for instance the procedure of determining and verifying digital signature. Here the digital signature would be substituted with a DNA signature which is individual for each man (except for monozygotic twins), and coded in the digital form. The DNA signature attached to a message that Alice is to send to Bob would guarantee that the text of the message is not modified and,

what is most important, it would authenticate the author. Such message would be sent via a fully secured channel that rules out eavesdropping (Krzyszkowska-Pytel, 2010).

A cryptographic digital key is generated from a biometric such as a fingerprint or voice and is used to sign transactions initiated by a relying party. Raw biometric data is never sent through the network or stored in a central database.

Biometric Encryption is an algorithm for the linking and retrieval of digital keys, which can be used as a method for the secure management of cryptographic keys. The cryptographic key is generated independently from the Biometric Encryption algorithm and can be updated periodically via a re-enrollment procedure. When crypto-biometric systems eventually come into practical existence, there is a danger that biometric components may be used as a certain proof of existence of a particular subject at a particular time and place. Mere incorporation of biometrics into a system does not in itself constitute a proof of identity. It needs to understand how these foolproof guarantees can be theoretically proved in a deployed cryptosystem and how to institute due processes that will provide both technological and sociological freedom to challenge the premises on which non-repudiation is ascertained.

The convenience and security provided by Biometric Encryption will undoubtedly help to promote more widespread use of cryptographic systems.

With respect to the design goals, BCSs offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level. Techniques which provide provable security/privacy, while achieving practical recognition rates, have remained elusive (even on small datasets). Additionally, several new issues and challenges arise deploying these technologies. One fundamental challenge, regarding both technologies, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within both technologies, i.e., alignment of obscured templates without leakage is highly non-trivial. While for some biometric characteristics (e.g., iris) alignment is still feasible, for others (e.g., fingerprints) additional information, which must not lead to template reconstruction, has to be stored. Within conventional biometric systems, align-invariant approaches have been proposed for several biometric characteristics. So far, hardly any suggestions have been made to construct align-invariant BCSs. Feature adaptation schemes that preserve accuracy have to be utilized in order to obtain common representations of arbitrary biometric characteristics (several approaches to extract binary fingerprint templates have been proposed, e.g., Meenakshi & Padmavathi, 2009; Kanade et.al., 2009; Cavoukian & Stoianov, 2009) allowing biometric fusion in a form suitable for distinct template protection schemes. Focusing on BCSs it is not actually clear which biometric characteristics to apply in which type of application. In fact it has been shown that iris or fingerprints exhibit enough reliable information to bind or extract sufficiently long keys providing acceptable trade-offs between accuracy and security, where the best performing schemes are based on fuzzy commitment and fuzzy vault. However, practical error correction codes are designed for communication and data storage purposes such as a perfect error correction code for a desired code length has remained evasive. In addition, a technique to generate chaff points that are indistinguishable from genuine points has not yet been proposed. The fact that false rejection rates are lower bounded by error correction capacities emerges a great challenge since unbounded use of error correction (if applicable) makes the system even more vulnerable (Chen, Sun, & Lam, 2007; Stoianov et.al., 2009; Monrose, Reiter, & Wetzel, 1999). Other characteristics such as voice or keystroke dynamics (especially behavioral characteristics) were found to reveal only a small amount of stable information, but can still be applied to improve the security of an existing secret (Monrose, Reiter, & Wetzel, 1999; Monrose et. al., 2001; Chafia, Salim, & Farid, 2010).

In addition, several characteristics can be combined to construct multi-BCSs (Voderhobli, Pattinson, & Donelan, 2006), which have received only little consideration so far. Thereby security is enhanced and feature vectors can be merged to extract enough reliable data.

While for some characteristics, extracting of a sufficient amount of reliable features seems to be feasible it still remains questionable if these features exhibit enough entropy. In case extracted features do not meet the requirements of discriminability, systems become vulnerable to several attacks (e.g., false acceptance attacks). In addition, stability of biometric features is required to limit information leakage of stored helper data. Besides, several specific attacks to BCSs have been proposed. While key approaches have already been exposed to fail high security demands, more sophisticated security studies for all approaches are required since claimed security of these technologies remains unclear due to a lack formal security proofs and rigorous security formulations (Voderhobli, Pattinson, & Donelan, 2006).

References

An Introduction to Cryptography, (1990-2000). Network Associates, Inc. and its Affiliated Companies. http://www.nai.com

Adler, A. (2004). *Images can be Regenerated from Quantized Biometric Match Score Data*, Proceedings of the Canadian Conference on Electrical and Computer Engineering, Niagara Falls, Canada, 469-472

Adler, A. (2005). *Vulnerabilities in biometric encryption systems*, School of Information Technology and Engineering, University of Ottawa, Ontario, Canada

Adler, A. (2008). *Biometric System Security*, Systems and Computer Engineering, Carleton University, Ottawa, Canada

Bergamo, P., D'arco, P., Santis, A. D., & Kocarev, L. (2005). *Security of Public Key Cryptosystems based on Chebyshev Polynomials*

Boyen, X. (2004). *Reusable cryptographic fuzzy extractors*, Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS '04), 82-91, Washington, DC, USA

Boult, T. E., Scheirer, W. J., & Woodwork, R. (2007). *Revocable fingerprint biotokens: accuracy and security analysis*, Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '97), 1-8, Minneapolis, Minn, USA

Cavoukian, A., Stoianov, A. (2009). *Biometric encryption: the new breed of untraceable biometrics*, Biometrics: Fundamentals, Theory, and Systems Wiley, London

Cavoukian, A. & Stoianov, A. (2007). *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security, and Privacy*, http://www.ipc.on.ca

Chen, H., Sun, H., Lam, K. Y. (2007). *Key management using biometrics*, Int Symposium on Data, Privacy, and E-Commerce, 1:321-326

Chafia, F., Salim, C., & Farid, B. (2010). *A biometric crypto-system for authentication*, Proceedings of Int Conf on Machine and Web Intelligence (ICMWI), 434-438

Dijk, M. V., & Tuyls, P. (2005). *Secure Biometrics*, Philips Research Laboratories Prof. Holstlaan 4, AA 5656 Eindhoven, The Netherlands

Davida, G. I., Frankel, Y., & Matt, B. J. (1998). *On enabling secure applications through off-line biometric identification*. In Proceedings of the 1998 IEEE Symposium on Security and Privacy, 148-157

Enayah, M. R., & Samsudin, A. (2007). *Securing Telecommunication based on Speaker Voice as the Public Key*, IJCSNS International Journal of Computer Science and Network Security, Vol.7, Issue 3

Fabian M., Michael K. R., Qi L. & Susanne W. (2001). Cryptographic Key Generation from Voice, Proceedings of the 2001 IEEE Symposium on Security and Privacy

Grindlay, B. (2013). *Quantum Cryptography: A study into the present technologies and future applications*, Next Generation Security Software Ltd, www.ngssoftware.com

Goh, A., & Ngo, D. C. L. (2003). *Computation of cryptographic keys from face biometrics*. In Proceedings of Communications and Multimedia Security, 1-13

Hao, F., Anderson, R., & Daugman, J. (2006). *Combining cryptography with biometrics effectively*, IEEE Transactions on Computers, Computer Laboratory, Cambridge University, UK

Hao, F., & Wah, C. (2002). *Private key generation from on-line handwritten signatures*, Information Management and Computer Security 10, Vol. 4, 159-164

Jain, A. K., Ross, A., & Uludag, U. (2005). *Biometric Template Security: Challenges and Solutions*, Proceedings of European Signal Processing Conference (EUSIPCO)

Jain, A. K., Nandakumar, K., & Nagar, A. (2008) *Biometric Template Security*, Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 579416

Juels, A., & Wattenberg, M. (1999). *A fuzzy commitment scheme*, ACM Conference on Computer and Communications Security, 28-36

Jules, A., & Sudan, M. (2006). *A Fuzzy Vault Scheme,* Springer Science+Business Media, Inc. Manufactured in The United States

Juels, A., & Sudan, M. (2006). *A fuzzy vault scheme*. Des. Codes Cryptography, 38(2):237-257

Kanak, A. (2004). *Biometrics For Computer Security And Cryptography*, Gebze Yüksek Teknoloji Enstitüsü

Kanade, S., Camara, D, Petrovska-Delacrtaz, D., & Dorizzi, B. (2009). *Application of biometrics to obtain high entropy cryptographic keys*, Proceedings of World Academy on Science, Engineering, and Technology, Hong Kong

Krzyszkowska-Pytel, M. (2010). *Quantum Cryptography – The Issue of Security in Selected Quantum Protocols and the Issue of Data Credibility*, Theoretical and Applied Informatics, ISSN 1896–5334, Vol. 22, Issue 1, 73–92

Linnartz, J. P., & Tuyls, P. (2003). *New shielding functions to enhance privacy and prevent misuse of biometric templates*, Audio and Video-Based Biometric Person Authentication, 393-402

Meenakshi, V. S., & Padmavathi, G. (2009). *Security analysis of password hardened multimodal biometric fuzzy vault*, Proceedings of World Academy of Science, Engineering and Technology, 56

Monrose, F., Reiter, M. K., & Wetzel, S. (1999). *Password hardening based on keystroke dynamics*, Proceedings of 6th ACM Conf on Computer and Communications Security, CCCS, 73-82

Monrose, F., Reiter, M. K., Li, Q., & Wetzel, S. (2001). *Cryptographic key generation from voice*, SP '01: Proc of the 2001 IEEE Symp on Security and Privacy, 12

Monrose, F., Reiter, M. K., Li, Q., & Wetzel, S. (2001). *Cryptographic key generation from voice* (extended abstract), Proceeedings of the 2001 IEEE Symposium on Security and Privacy, 12-25

Monrose, F., Reiter, M., Li, Q., Lopresti, D., & Shih, C. (2002). *Towards speech-generated cryptographic keys on resource-constrained devices*, Proceedings of the Eleventh USENIX Security Symposium, 283-296

Nandakumar, K., Nagar, A., & Jain, A. K. (2007). *Hardening fingerprint fuzzy vault using password*, Proceedings of 2nd International Conference on Biometrics, 927-937, Seoul, South Korea

Ratha, N. K., Connell, J.H., & Bolle, R.M. (2001). *Enhancing security and privacy in biometrics-based authentication systems*, IBM Syst J 2001, 40:614-634

Savvides, M., Kumar, B., Khosla, P. (2004). *Cancelable biometric filters for face recognition,* ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04), 3:922-925

Scheirer, W. J., & Boult, T. E. (2007). *Cracking Fuzzy Vaults And Biometric Encryption*, Securics Inc. and University of Colorado at Colorado Springs Colorado Springs, CO.

Soutar, C., & Tomko, G. J. (1996). *Secure private key generation using a fingerprint*, Cardtech/Securetech Conference Proceedings, 245-252

Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., & Kumar, B. V. (1998). *Biometric encryptiontm using image processing,* Optical Security and Counterfeit Deterrence Techniques II, Vol. 3314, IS&T/SPIE, 178-188

Stoianov, A,, Kevenaar, T., & van der Veen, M. (2009). *Security issues of biometric encryption,* Proceedings of the Toronto Int. Conf. Science and Technology for Humanity (TIC-STH), 34-39

Sutcu, Y., & Li, Q., & Memon, N. (2007). *How to Protect Biometric Templates*

Teoh, A. B. J., Kuan, Y. W., & Lee, S. (2008). *Cancellable biometrics and annotations on biohash*, Pattern Recognition, 41(6):2034-2044

Tuyls, P., & Goseling, J. (2004). *Capacity and Examples of Template-Protecting Biometric Authentication Systems*, Philips Research, Prof. Holstlaan 4, 5656 AA Eindhoven, The Netherlands

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004) *Biometric cryptosystems: Issues and challenges*, Proceedings of the IEEE: Special Issue on Multimedia Security of Digital Rights Management 92, Vol. 6, 948-960.

Uludag, U., & Jain, A. (2004). *Attacks on biometric systems: A case study in fingerprints*, Proceedings of SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, Vol. 5306, 622-633

Uludag, U., & Pankanti, S., & Jain, A. K. (2005). *Fuzzy vault for fingerprints*, AVBPA, 310-319

Uludag, U., & Jain, A. K. (2006). *Securing fingerprint template: Fuzzy vault with helper data*, Privacy Research in Vision, 163

Uludag, U., & Jain, A. (2006). *Securing fingerprint template: Fuzzy vault with helper data*, Proceedings of the IEEE Workshop on Privacy Research in Vision (PRIV), New York, NY

Vielhauer, C., Steinmetz, R., & Mayerhofer, A. (2002). *Biometric hash based on statistical features of online signatures*, Proceedings of the Sixteenth International Conference on Pattern Recognition, Vol. 1, 123-126

Vielhauer, C., & Steinmetz, R. (2004). *Handwriting: Feature correlation analysis for biometric hashes*, EURASIP Journal on Applied Signal Processing 4, 542-558

Voderhobli, K., Pattinson, C., & Donelan, H. (2006). *A schema for cryptographic key generation using hybrid biometrics*, 7th annual postgraduate symp.: The convergence of telecommunications, networking and broadcasting, Liverpool

Wayman, J. (2001). *Fundamentals of biometric authentication technologies*, International Journal of Image & Graphics, 93-114

Yamazaki, Y., Nakashima, A., Tasaka, K., & Komatsu, N. (2005). *A study on vulnerability in online writer verification system*, Proceedings of the Eighth International Conference on Document Analysis and Recognition, Seoul, South Korea, 640-644

Zhe, J., Andrew, B. J. T., Bok-Min, G. & Yong-Haur,T. (2016). *Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation*, ELSEVIER Pattern Recognition, Vol. 56, 50-62, https://doi.org/10.1016/j.patcog.2016.02.024

Zheng, G., Li, W., & Zhan, C. (2006). *Cryptographic key generation from biometric data using lattice mapping*, ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition, Washington, DC, USA, IEEE Computer Society, 513-516

Zhou, X. (2007). *Template Protection and its Implementation in 3D Face Recognition Systems*, Fraunhofer IGD, Fraunhoferstr. 5, 64283 Darmstadt, Germany

Zuo, J., Ratha, N. K., & Connel, J. H. (2008). *Cancelable iris biometric*, Proceedings of the 19th Int. Conf on Pattern Recognition (ICPR'08), 1-4

Mohamed SOLTANE (Prof. Dr.) received the M. Eng. degree in Electronics from Badji-Mokhtar University of Annaba, Algeria, in 1995 and the M. Sc. degree in Electrical and Electronics Engineering from National University of Malaysia in 2005, and the Ph. D. degrees in Electronics and Computer Engineering from Badji-Mokhtar University of Annaba, Algeria, in 2010. He is currently an Associate Professor at Electrical Engineering & Computing Department, Faculty of Sciences & Technology, Yahia Fares University Of Medea, Algeria. His research interests include statistical pattern recognition, biometric authentication, cryptography and quantum computing, computer vision and machine learning and microcomputer based system design.

Lotfi MESSIKH (Prof. Dr.) is a professor at Faculty of Engineering Sciences, University of Skikda, Algeria. He holds PhD in signal processing from the University of Badji Mokhtar Annaba, Algeria. His research interest focus on signal processing, automatic speech processing and system design for photovoltaic applications.

Abdelhalim ZAOUI (Prof. Dr.) is a professor with the Electrical Engineering Research UNIT, MPS, Algiers, Algeria.